Aufgabe 3

Der folgende Text ist mithilfe des Vigenère-Verfahrens mit dem Schlüsselwort GELD chiffriert worden:

```
YTLUQ EDVKE XPGVV WAQKZ KMFKX
```

a) Erläutern Sie das Vigenère-Verfahren und dechiffrieren Sie den Text.

Ein gewöhnlicher deutscher Text wurde auf zwei verschiedene Arten chiffriert. Im Material finden Sie die beiden Chiffrate. Außerdem sind die relativen Häufigkeiten der fünf am häufigsten vorkommenden Zeichen angegeben.
Ordnen Sie die beiden Chiffrate jeweils einem klassischen Chiffrierverfahren begründet zu.

b) Im Material sind Fragmente einer Java-Klasse bzw. eines Delphi-Programms zu finden, mit der ein gegebener Text mithilfe des Vigenère-Verfahrens chiffriert werden kann.
Ergänzen und kommentieren Sie die Operation `chiffriere`.

e) Von einem längeren mithilfe des Vigenère-Verfahrens chiffrierten Text ist nur die Länge des Schlüsselwortes bekannt. Erläutern Sie Möglichkeiten der Kryptoanalyse.
Beurteilen Sie die Sicherheit des Vigenère-Verfahrens.

Zu Aufgabe 3a)

Erster chiffrierter Text

```
YDTYUIUHQK VWQRUWUXJU IKCTUDKDJU HISXYUTPMY ISXUDUYDUH
CEDEQBFXQR UJYISXUDKD TUYDUHFEBO QBFXQRUJYI SXUDLUHISX
BKUIIUBKDW TYUIURUYTU DWHKDTIQUJ PBYSXLUHIS XYUTUDUDLU
HVQXHUDIEB BUDXYUHTYI AKJYUHJMUH TUDISXKUBU HKDTISXKUB
UHYDDUDTYU IYSXWKJQKV TYUQRYJKHA BQKIKHLEHR UHUYJUJXQR
UDIEBBJUDT QCYJQRUHAU YDUISXMYUH YWAUYJUDXQ RUDMUHDYSX
JWUDKWWUBU HDJXQJAQDD IYSXQDTYUI UHQKVWQRUT YUPQUXDUQK
IRUYIIUDRU XQDTUBJMKH TUTYUIUIJX UCQRUHUYJI YDTUHZQXHW
QDWIIJKVUP MEUBVKDTXQ JIYSXUHBYS XTUDISXKUB UHDKDTISXK
UBUHYDDUDL YUBUDUKUYD VEHCQJYEDU DWUBYUVUHJ LYUBUHVEBW
```

Häufigste Zeichen: U: 19,0 % D: 9,8 % Y: 8,4 % H: 6,6 % I: 6,6 %

Zweiter chiffrierter Text

```
IOLBYJESIN ZXACMZYYTF ANGUEOCGNV RTKACVDAEB MTHFVXCEES
UHHFAMXAUS EUQLWYEOCG XVIOMKJFLZ IEJYACMMCJ CIMGPVRTKA
FLETAXFLNH LBYJECMBXV NHZNHUSBMM TCIDPOYISD PBYUEOMGPV
RGIALVNTWE FVNIQXLUIT SNNZESBPYI DFVLWYUFTX LLNEAVBLEM
MKCENFVWCV SJKAALTBCY XZEBJBNLRL TTOJUSDHLS ESMBNVTIIU
YESPTENVNE IFCKACMKEV IOMLWYWJMK CXKFQMYEHB JXHNESVBWY
THMGOXGFTX LETIIMERNO ABWYAOLBYJ ESINZXACMW CVZBMAHVAV
AUYZSTMGVV HBVWYCTXCK XVDJMLYJTI MFUSESMBNJ IOLXLAAIZZ
UEGTAMOWEA EHYCFVVWBR TTQVBVRMQV BUEOAVBLEM MKHLNEAVBL
EMMKCENFVO CVLFVXOVIO NHLDAUQHHV NHMECVFFZM PZEMMKZFLH
```

Häufigste Zeichen: E: 7,6% V: 7,4% M: 7,2% L: 5,6% A: 5,4%

Zu Aufgabe 3b)

Java-Programmfragment:

```
public class vigenere {

  static String klarText;
  static String geheimText;
  static String schluessel;

  static void textEinlesen() {
    // Der zu verschlüsselnde Text wird eingelesen
    // und in der String-Variablen  klarText  gespeichert.
  }

  static void schluesselEinlesen() {
    // Der Schlüssel wird eingelesen
    // und in der String-Variablen  schluessel  gespeichert.
  }

  static void textAusgeben() {
    // Der in der String-Variablen geheimText  gespeicherte Text wird ausgegeben.
```

```
  }

  static void chiffriere() {

    // hier muss ergänzt werden .....

  }

  public static void main(String[] args) {
    textEinlesen();
    schluesselEinlesen();
    chiffriere();
    textAusgeben();
  }
}
```

Delphi-Programmfragment:

```
program vigenere();

var klarText:string;
    geheimText:string;
    schluessel:string;


procedure textEinlesen;

  // Der zu verschlüsselnde Text wird eingelesen
  // und in der String-Variablen  klarText  gespeichert.


procedure schluesselEinlesen;
  // Der Schlüssel wird eingelesen
  // und in der String-Variablen  schluessel  gespeichert.


procedure textAusgeben;
  // Der in der String-Variablen  geheimText  gespeicherte Text wird
  // ausgegeben


procedure chiffriere;
begin

  // hier muss ergänzt werden .....

end;

procedure TForm1.FormCreate(Sender: TObject);
begin
  textEinlesen;
  schluesselEinlesen;
  chiffriere;
  textAusgeben;
end;
```

Vigenère-Tafel

0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y